DOD Computer Network Operations: Time To Hit The Send Button

By Joseph Glebocki, Jr., Lieutenant Colonel, USAF

Editorial Abstract: Lt Col Globecki analyzes the current DOD cyber security role, particularly as it applies in support of US Military Assistance to Civil Authority. He examines the impact of the Posse Comitatus Act, and how some interpretations unnecessarily hinder a cooperative effort to protect US critical infrastructure.

Terrorists in a cyber café in Kansas City, Missouri, infiltrate Department of Defense (DOD) computer networks and unleash a malicious virus that shuts down US missile defense systems, leaving the United States vulnerable to an intercontinental ballistic missile attack.

Besides defensive measures aimed at protecting its systems from further damage, DOD remains extremely vulnerable—there is not much else that it can do without the help or acquiescence of federal civilian authorities. In the meantime, lives could be lost, cities destroyed, and the American way of life could be changed forever. Although this is a hypothetical scenario that sounds like a science fiction thriller, such unthinkable events could happen in the future if US law and policy are not changed to enable DOD to fully defend and fight in cyberspace. Clearly, DOD is moving into the cyber domain of warfare, but the US Government will not be ready to exploit its full potential until DOD is given the tools and the authorities to become more aggressive in cyberspace to perform these evolving cyber missions when necessary, before it is too late.

Legal and policy barriers against the use of DOD resources from the outset to defend and then respond to cyber attacks against US national infrastructure can severely hamper its homeland security posture. With the United States facing national security threats at home and abroad like never before, this article advocates that it is time to provide a new policy and legal regime for cyber offense and defense.

The Cyber Threat to US Critical Infrastructure

Cyberspace is a difficult concept to define, since it might mean something different depending upon the context. The official DOD definition provides that cyberspace is the notional environment in which digitized information is communicated over computer networks. Regardless of how we define it, there can be little debate over the potential vulnerability of our networked systems. The *National Infrastructure Protection Plan* (NIPP) recognizes US economy and national security are highly dependent upon the global cyber infrastructure, creating a highly interconnected and interdependent network of Critical Infrastructure/Key Resources (CI/KR). Although new technologies and interconnected networks enhance productivity and efficiency, they also serve to increase America's risk to cyber threats. For example, "[t]he expansive growth of new Internet technologies, from wireless access to voice-over-Internet telephony, has engendered new threats that have been outpacing the security responses of private and governmental users on the whole." One of the great advantages of cyberspace is anonymity, plus the ability to undertake attacks remotely in an almost untraceable way, while using third party computer systems, and often with minimal risk of detection or retaliation.

Despite extensive government and private industry efforts, the Computer Emergency Response Team (CERT) Coordination Center list of reported vulnerabilities grew from about 2,500 in 2001 to more than 7,200 in 2006—about 20 new vulnerabilities every day. Similarly, an August 2005 International Business Machines (IBM) report showed more than 237 million computer security attacks reported worldwide in the first half of 2005, with US Government organizations being the most likely target by far. One can only imagine how many attacks must go undetected. General James Cartwright, then USSTRATCOM Commander, warned in a March 2007 statement to the House Armed Services Committee that "America is under widespread attack in cyberspace. Unlike air, land, and sea domains, we lack dominance in cyberspace, and could grow increasingly vulnerable if we do not fundamentally change how we view this battlespace."

The scope of enemies in this domain is potentially limitless: traditional hostile countries trying to gain information on our military capabilities; malicious individual hackers looking to steal valuable information from the federal government; terrorists; criminal elements; and even economic competitors. Retired General Barry McCaffrey stated "every classified brief I receive underscores the absolute certainty that all our potential adversaries, terrorist organizations, and many private criminal groups conduct daily electronic reconnaissance and probes of the electromagnetic spectrum and devices which are fundamental to our national security." The Federal Bureau of Investigation (FBI) even predicts terrorists could use hackers to conduct cyber attacks to complement large scale conventional attacks.

Similarly, the US *National Military Strategy* contends that cyber attacks on US commercial information systems or transportation networks could conceivably have a greater economic or psychological effect than a Weapons of Mass Destruction (WMD) attack. It is well-documented that "increasingly sophisticated use of the Internet and media has enabled our terrorist enemies to communicate, train, rally support, proselytize, and spread their propaganda without risking personal contact." The *National Strategy for Combating*

Terrorism seeks to eliminate such "cyber safehavens" because the Internet provides an inexpensive, anonymous, geographically unbounded, and largely unregulated virtual safe haven for extremists. Such activities will have a much higher future likelihood of success if the US restricts DOD from conducting robust counterattacks and offensive operations in cyberspace.

Impact of the Posse Comitatus Act

Despite the growth of cyber-based threats to US national security and critical infrastructure, the *Posse Comitatus Act* (PCA) continues to serve as a significant potential roadblock to DOD's dominance in the cyberspace domain. The PCA provides in pertinent part: *"whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."* In general, the statute makes it a crime for the military to execute the laws of the United States, specifically performing domestic civilian law enforcement functions. Originally, the PCA prohibited the use of the Army as a posse comitatus, arising from the end of Civil War reconstruction and conditions throughout the US western frontier. The Act's prohibitions do not apply to members of the military reserves when not on active duty status, members of the National Guard when not in Federal service, civilian employees of DOD; the US Coast Guard when not employed under DOD, nor military members in an off-duty and private capacity.

The courts have come up with at least three different legal standards when discussing potential violations of the PCA; however, there is general agreement that passive law enforcement assistance is permitted. In *United States versus Red Feather*, the District Court delineated the general standard of permissible passive roles and impermissible active roles. In another case, the Court stressed whether the use of any part of the military pervaded the activities of federal law enforcement officers. Another Federal District Court decision came up with the third standard, which asks if military personnel subjected citizens to an exercise of military power that was regulatory, proscriptive, or compulsory in nature.

The Defense Department basically adheres to each of the three generally enunciated judicial standards, as well as any Congressional restrictions on military participation in civilian law enforcement activities. However, DOD appears to specifically endorse the third test in defining permissible activities, while adding express prohibitions on direct assistance, against searches and seizures, surveillance of individuals, or acting as an undercover agent or interrogator. The Justice Department's Legal Counsel uses a hybrid of the first and third tests when judging military activities against a standard of whether "there is no contact with civilian targets of law enforcement, no actual or potential use of military force, and no military control over the actions of civilian officials."

Who is keeping an eye on our critical infrastructure? (Defense Link)

From a legal analysis standpoint, the jury is probably still "out" as to whether *all* types of DOD responsive and offensive cyberspace operations would violate the PCA. Both sides make strong arguments. It also appears that the Department of Justice (DOJ) standard would not be violated, since there does not need to be contact with civilian targets of law enforcement, no use of military force in the traditional sense, and no military control over civilian officials. One can further argue the "military purpose" doctrine would be satisfied whenever protection of DOD critical infrastructure and equipment serves as the supporting rationale. Regardless of the legal scholars' conclusions, there is still too much uncertainty in the current state of the law to be of much value.

Exceptions to the PCA

The debate over the proper role of the military on the domestic front continues to be a hot topic since 9/11 and Hurricane Katrina (2005). Nonetheless, the US Congress reaffirmed its support for the PCA by stressing its continued importance, stating it has served the nation well. However, the US Congress also makes it clear the PCA is not a complete barrier to use the Armed Forces for a range of domestic purposes, including law enforcement. In fact, the statute has already been amended many times, creating numerous exceptions that dilute the scope of the law.

Exceptions to the PCA fall in four major areas: insurrections/ civil disturbances, counterdrug operations, disaster relief, and counterterrorism/ weapons of mass destruction. PCA language contains a clear exception clause for "circumstances expressly authorized by the Constitution or Act of Congress." Furthermore, it offers some discretion in situations where an immediate response is necessary for temporary emergencies, when the local authorities are overwhelmed. Most importantly, statutory law provides that assistance in the context of a WMD attack may include use of DOD personnel to arrest persons and conduct searches and seizures, with respect to violations of this section. Even direct military assistance is permitted in limited circumstances, with the two major exceptions being the *Military Purpose Doctrine* and the *Insurrection Act*.

Yet laws that allow the military to help address the problems of drug trafficking, natural disasters, and terrorist

attacks have consistently weakened the Act. Some of the PCA's biggest changes came after President Reagan's "War on Drugs" in the 1980s. After powerful testimony by state and local leaders requesting military assistance, Congress pushed DOD to provide indirect assistance to law enforcement including: intelligence, equipment, maintenance, use of military facilities, plus specialized training and tactical advice. In addition to modern challenges faced by law enforcement, the President's Constitutional and statutory authorities have further eroded PCA prohibitions. With so many exceptions already in place, is there really a need for the PCA in today's dangerous environment—considering the cyberspace threat we already face?

If the US maintains the current PCA structure, Congress should create a new exception allowing DOD to fully defend itself against cyber attacks, and properly respond to the growing threat. Since Congress has already provided DOD with "police powers" in the context of WMD incidents, it would not be a stretch to extend this policy to cyberspace. Although the law is still relatively new in this area, there are strong arguments that a search and seizure has taken place whenever the government conducts cyberspace investigations relating to personal and business network servers. However, this is the only way for DOD to be able to protect US national security interests. Such activities should be even less visible—and hopefully less objectionable—than having military forces on the streets during civil disturbances or border patrol operations.

National Critical Infrastructure Protection (CIP)

The President's Commission on Critical Infrastructure Protection (PCCIP), created by the Clinton administration, was charged with reviewing all national critical infrastructure physical and cyber threats. In *Presidential Decision Directive* (PDD)*/NSC-63*, the President stated "…the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both

physical and cyber attacks on our critical infrastructures, including especially our cyber systems." This Directive's national goals state interruptions or manipulations of critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to US welfare. The associated guidelines provide the authorities, capabilities and resources of the US Government—including defense preparedness—to achieve and maintain critical infrastructure protection. Further, every federal department is responsible for protecting its own critical infrastructure and cyber-based systems.

One major challenge was the development of a system for responding to significant infrastructure attacks already underway, with the goal of isolating and minimizing damage. The National Infrastructure Protection Center (NIPC) was supposed to provide the principal means of facilitating and coordinating the overall response, mitigating attacks, investigating threats, and monitoring reconstitution efforts, while maintaining that foreign attacks could place them in a direct support role to DOD. The National Cyber Security Division (NCSD), part of DHS' Preparedness Directorate, provides the federal government with a centralized cyber security coordination and preparedness function. NCSD further serves as the focal point for interactions with state and local government, the private sector, and the international community regarding cyberspace vulnerability reduction. Under the *National Response Plan's* Cyber Annex, the National Cyber Response Coordination Group (NCRCG) is designated as the main interagency mechanism to prepare for and respond to cyber incidents of national significance. Among its duties, NCRCG leverages the capabilities of US Government agencies from a cyber defense perspective, providing situational awareness to detect and recognize incidents of significance. Further, NCRCG is tasked to attribute the source of attacks and malicious activity, coordinate responses, and help with the recovery of potential disruptions.

The National Strategy to Secure Cyberspace

Securing cyberspace is a difficult strategic challenge, requiring coordinated and focused efforts from our entire society: the federal government; state and local governments; the private sector; and the American people. The *National Strategy to Secure Cyberspace* has three strategic objectives: preventing cyber attacks against America's critical infrastructures; reducing national vulnerability to cyber attacks; and minimizing damage and recovery time from cyber attacks that do occur. It also identifies six major actions and initiatives to strengthen our national security and international cooperation including:

1. Strengthening cyber-related counterintelligence efforts;
2. Improving capabilities for attack attribution and response;
3. Improving coordination for responding to cyber attacks within the US national security community;
4. Fostering the establishment of national/international "watch" and "warning" networks to detect and prevent emerging cyber attacks.

Another important policy document, *Homeland Security Presidential Directive (HSPD)-7*, establishes a national policy for federal departments and agencies to identify and prioritize CI/KR and to protect them from terrorist attacks. Some of the major difficulties with protecting these areas: most are privately owned and operated; most include cyber-based resources; and most span all sectors of our economy. HSPD-7 states it is

US policy to enhance protection of the country's critical infrastructure and key resources against terrorist acts that could:

1. Impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;

2. Undermine State and local government capabilities to maintain order and to deliver minimum essential public services;

3. Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

4. Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources;

5. Undermine the public's morale and confidence in our national economic and political institutions.

The Secretary of Homeland Security has the apparent responsibility to coordinate the overall national effort, and to serve as the lead federal official. In addition, the Secretary is directed to maintain an organization to serve as the focal point for cyber security, with DOD and other organizations collaborating and supporting this overall mission as necessary under current law. The DOD is specifically designated with lead responsibility for the defense industrial base. DHS established the United States Computer Emergency Readiness Team (US-CERT) as the 24/7 single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery operations through partnerships between DHS and the public and private sectors to protect the national cyber infrastructure. Further, the *National Infrastructure Protection Plan* (NIPP) promotes cyber security by facilitating participation and partnership in CI/KR protection initiatives, leveraging cyber-specific expertise and experience, and improving information exchange and awareness of cyber security concerns. The resulting framework enables security partners to work collaboratively in making informed cyber risk management decisions, defining national cyber priorities, and addressing overall cyber security.

Critical infrastructure connects us all. (US Air Force)

DOD Capabilities and Policies

In February 2003, President Bush provided classified guidance, NSPD-16, to determine how and when the United States would launch a Computer Network Attack (CNA) against foreign systems, and who would be authorized to conduct such operations. Due to many uncertainties in the cyberspace realm, DOD recommended a legal review to determine what level of cyber intrusion amounts to an actual attack; whether the response could infiltrate unknowing third party systems; and an overall framework that might apply separately to domestic or foreign attackers. Clearly, there is much in the area of policy and law the US must resolve at the national and DOD levels before taking a final course of action. Yet, DOD officially acknowledges that cyberspace is considered a warfare domain just like air, land, sea, or space.

Cyberspace is also recognized as a new theater of operations by the *National Defense Strategy* because successful military operations depend upon the ability to protect information infrastructure and related data. However, DOD leadership knows that it will take time for our military forces to adapt to this new way of warfare: it has no "battle lines;" intelligence is intangible; and attacks come without warning, leaving no time to prepare defenses. DOD states it is building an information-centric force, with networks increasingly recognized as operational centers of gravity—so it must be prepared to "fight the net." However, "current US cyber warfare strategy is dysfunctional… resulting in a disjointed effort," argued General James Cartwright, former Commander of STRATCOM. Ultimately, the Secretary of Defense has the responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support military operations.

Current DOD Organization

The Unified Command Plan (UCP) assigns USSTRATCOM as the DOD lead for Computer Network Operations (CNO). The Joint Functional Component Command Network Warfare (JFCC-NW), a subordinate command of USSTRATCOM, serves as the lead for coordinating DOD network warfare. The Joint Task Force for Global Network Operations (JTF-GNO) is responsible for operating and defending US worldwide information networks associated with the Global Information Grid (GIG). Established Computer Network Defense (CND) policy includes three tiers of response actions, with corresponding levels of approval authority up to Tier 1, which includes STRATCOM being authorized to take defensive measures and actions that may "minimally and temporarily adversely affect adversary systems and may have a similar affect upon intermediate systems." However, it is apparent that CND lacks any updated policy and legal guidance to adequately guide responses to attacks against DOD networks.

Although any aspects of Computer Network Attack (CNA) and its implementing organizations are likely to be highly classified, it is generally believed that the US can actually destroy networks and penetrate enemy computers to take data and disable command and control networks in an interagency framework. General Barry

McCaffrey states "we must sort out clearly the international legal and policy considerations upon which we will base widely understood Joint Directives governing the centralized employment of offensive cyber-warfare. This is the first sword to unsheathe in time of modern combat." Reportedly, the United States did *not* use CNA during Operation Iraqi Freedom, even with comprehensive information operations plans in place, perhaps since top-level approval was not granted in sufficient time to support campaign objectives.

Clearly, CNO mission areas are growing more important as DOD becomes increasingly dependent upon computer systems and networks to support our warfighters. Many DOD capabilities could be degraded if adversary military groups or terrorists were able to conduct sustained cyber attacks against DOD infrastructure. Within the United States, DOD would be unable to fully defend and respond to these threats without changes to the current policy framework. Furthermore, DOD's homeland defense and homeland security missions, including "sovereignty protection" and protection of defense critical infrastructure, could be unduly hampered. DOD has invested significant manpower and resources to address the cyber-based threat, with STRATCOM and its Service components primed to respond. In many cases, DOD has expertise that exceeds what is available in the civilian arena. With the stakes so high it does not make sense to leave the military as a reserve force, or to only "break the glass," when civilian authorities make a specific requests—or are already overwhelmed.

Accordingly, DOD should serve as the lead: its mission can be focused upon the cyber defense of defense critical infrastructure and the corresponding response, as well as responding to cyber attacks that seriously degrade other national critical infrastructure. We can draw an analogy to defending US airspace from enemy aircraft, as well as hijacked aircraft already within our airspace, as demonstrated by the 9/11 attacks. There can be no differentiation between threats emanating from within and outside the US, because the risk of potential devastation is too great. Just as NORTHCOM and NORAD provide defense of our sovereign airspace, using Service component assets, and with full cooperation of civil authorities—the same should be done for cyberspace. The US Government will have to determine a set of protocols, and make this determination as expeditiously as possible. Two potential standards for DOD's cyber response are within the DOD *Strategy for Homeland Defense and Civil Support*, and HSPD-7 policy. If the New York Stock Exchange was struck by a cruise missile from another country and severely damaged, a military response would certainly be warranted. It should be no different if a cyber attack from that same state resulted in a similar level of devastation. DOD should be able to respond in a timely and effective manner to protect and serve US national interests, even when the national critical infrastructure in question belongs to the private sector.

"DOD is focused on cyber defense…"
(Defense Link)

To achieve success in the long run, the US will need to develop better capabilities to determine the second, third, and even higher order effects of offensive cyber operations, while minimizing outside disruptions to the greatest extent possible. Certainly we must also address potential discrimination and proportionality issues related to the law of war. It will be necessary for the international community to get together and work out many of these cyber warfare issues. Even when the source location of the attack is known, controversial matters will need resolution. If a foreign state is the attacker, and DOD response is certainly warranted, then DOD should always serve as the lead. In fact, PDD/NSC-63 provides that foreign cyber attacks could place the NIPC and other civilian agencies in a direct DOD support role. Of course, the US Government would still need to determine what level of cyber attack can be considered an act of war or aggression by another state. If a foreign-based extremist conducts the attack, the same rationale applies, although some might argue the FBI or CIA should handle the response. If the actor is a domestic terrorist, or US citizen hacking from within our own borders, we face the most difficult problem resolution due to domestic legal requirements. Nonetheless, DOD should still serve as the lead when the attack targets defense critical infrastructure, or when other national critical infrastructure is seriously degraded. These operations should not impact the capability of federal civilian authorities to prosecute the perpetrators in a court of law.

Military Assistance to Civil Authorities (MACA)

Under the heading of civil support, employment of military forces within the US borders typically falls under the broad mission of MACA. This construct includes three main areas:

1. Military support to civil authorities (MSCA);
2. Military support to civilian law enforcement (MSCLE);
3. Military assistance for civil disturbances.

DOD Directive 3025.15 establishes policy and assigns responsibilities for providing military assistance to civil authorities. The Directive defines MACA as activities and measures covered under MSCA plus DOD assistance

for civil disturbances, counter drug, sensitive support, counterterrorism, and law enforcement. It further provides that DOD "… shall cooperate with and provide military assistance to civil authorities as directed by and consistent with applicable law, Presidential Directives, Executive Orders, and this Directive."

DOD employment within the United States is supposed to be heavily weighted toward managing the consequences of the terrorist threat or use of chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) WMD. In reality, this does not appear to be the case. All requests for DOD military assistance are evaluated against several criteria including legality, the potential use of lethal force, risk to military forces, impact on the defense budget, appropriateness for a DOD mission, and any effect on military readiness. DOD is supposed to always remain in support of a lead federal agency during both crisis management (FBI) and consequence management (FEMA), as delineated in the *Interagency Domestic Terrorism Concept of Operations Plan* and the *Federal Response Plan*.

Under the broad MACA umbrella, it is consistent with DOD policy to move more aggressively into defensive and offensive cyber space operations. There is no likelihood of lethal force, no risk to military forces, and probably little relative impact on the defense budget and military readiness.

Military Support to Civil Authorities

Military Support to Civil Authorities (MSCA) refers to DOD support in response to requests for assistance during domestic incidents such as terrorism, major disasters or other emergencies. DOD Directive 3025.1 governs MSCA for all DOD components and defines such actions as:

...those activities and measures taken by the DOD components to foster mutual assistance and support between the DOD and any civil government agency in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including national security emergencies. Military forces employed in MSCA activities shall remain under military command and control at all times and shall not perform any functions of civil government unless absolutely necessary on a temporary basis in certain emergency circumstances. The Secretary of Defense has the responsibility to develop regulations to ensure that these actions do not include or permit direct participation by Service members in searches, seizures, arrests or similar activities unless otherwise authorized by law.

MSCA in action: Air National Guard disaster response. (US Air Force)

Any military forces involved in responsive or offensive cyber activities would likely be performing such functions only when absolutely necessary, on a temporary basis, and in emergency circumstances. Of course, military personnel would need to be trained adequately to determine when it would be appropriate to respond to cyber attacks using some type of risk analysis and established minimum criteria such as those delineated in HSPD-7 or the *DOD Strategy for Homeland Defense and Civil Support*.

Military Support to Civilian Law Enforcement

Military Support to Civilian Law Enforcement (MSCLE) involves military forces supporting a lead federal agency during various events:

1. National security special events;
2. Support for combating terrorism;
3. Support to counterdrug operations; maritime security;
4. Intelligence, surveillance, and reconnaissance;
5. General support (such as training, equipping, advising).

It is DOD policy to cooperate with civilian law enforcement as much as possible while remaining consistent with the needs of national security and military preparedness, while maintaining the historic tradition of limited direct military involvement, plus and the requirements of applicable law. Arguably DOD cyber activities would not violate MSCLE directives when taken for the primary purpose of furthering a military function of the United States, or when taken to protect DOD classified information or materials. It is also unlikely civilian authorities would be capable of providing an adequate response to large-scale attacks against DOD cyber-based infrastructure. There are often access or classification issues involved, so it would not make sense to hand off these problems to civilian officials. However, military members will definitely need additional training in areas such as evidence collection, especially for cases subject to American criminal jurisdiction.

Lessons Learned From Cyberspace Exercises

In the last several years, military and civilian authorities have recognized significant challenges in the cyberspace realm, especially when diverse organizations must work together in response. In late 2002, the city of San Antonio, Bexar County, Texas, and the surrounding region conducted exercise, "Dark Screen," to test the ability of local, state, and federal organizations to respond to a cyberattack. In fact, after action reporting from this exercise found the issue of military participation

continuously presented more questions than answers. Participants had concerns over the PCA, numerous DOD regulations, and other federal statutes addressing military support to civilian authorities.

"CyberStorm," a 2006 cyber attack exercise led by DHS, highlighted gaps and shortcomings in response planning at all levels of government. Specifically, the use of classified information and networks made coordination among agencies, levels of government, and the private sector increasingly difficult. Cyberstorm was the first full-scale government-led cyber security exercise to examine response, coordination, and recovery mechanisms to a simulated cyber event, involving international, federal, state, and local governments, in conjunction with the private sector. This specific scenario simulated a significant widespread cyber campaign affecting critical infrastructure elements within the energy, information technology, transportation, and telecommunications sectors. The exercise had three main objectives: to disrupt specifically targeted infrastructure through cyber attacks; to hinder the government's ability to respond; and to undermine public confidence in the government's ability to provide essential services. As a result, it became clear that all players require more: additional standard operating procedures (SOPs) and contingency plans; additional clarification of roles and responsibilities; and more education, training and exercises.

The Central Intelligence Agency conducted its own cyber exercises, notably the 2005 "Silent Horizon," which examined a major cyber attack against the US. During this activity it became apparent that many defenses are controlled by civilian telecommunications interests. Another CIA-sponsored exercise, "Livewire," determined significant questions over the government's role depending on the source of the attacks— terrorists, foreign States, or private citizens—still remain.

These exercises provide concrete examples of the serious issues the US could face under the current convoluted regime, if a large-scale cyber attack took place. Valuable time would be lost as DOD and civilian officials determine their proper roles. One answer might be the use of National Guard members or civilians in each state, to avoid PCA restrictions, but this would be an inefficient and likely unsupportable solution. Clearly, civilian and military officials need to do more in preparing and responding to threats, but not at the cost of limiting DOD's capability to protect its mission critical systems in a timely and comprehensive fashion.

A More Active DOD Cyber Defense Role

The cyber attack threat to US critical infrastructure is well-documented, both here, and throughout many other sources. The US defense critical infrastructure and other national critical infrastructure (economic, communications, transportation) are too intertwined to permit "stovepipes" across the federal government, the private sector, and elsewhere. The US cannot afford to have an attack, like Russia's purported 2007 actions against Estonia, that shuts down sectors of the government. In addition, cyber security exercises consistently show that the United States is not prepared or properly organized to meet the growing threats from States, terrorists, criminal organizations, and individual hackers.

The US has made some progress with the framework laid out by the *National Strategy to Secure Cyberspace,* HSPD-7, the NIPP, and other relevant policy documents. In addition, the US Government has made significant investments in building a foundation of cyberspace capabilities. DHS, NCSD, NCRCG, and US-CERT provide vital information exchange, awareness of cyber security issues, and build important partnerships. Similarly, DOD has made great strides with STRATCOM, its subordinate commands (JTF-GNO and JFCC-NW), and numerous other agencies to address the new warfighting domain of cyberspace. Yet, all of these efforts may ultimately only amount to "window dressing" if the PCA and current US policy remain in effect.

PCA Structure: Too Complex and Unnecessary

The *Posse Comitatus Act* has been more symbolic than real, as evidenced by the many exceptions permitted by Congress, the Courts' lackadaisical approach toward the statute, and the lack of federal enforcement. While the PCA has been on the books for more than 120 years, there has never been an actual prosecution for violating its provisions. Leaders from the Executive and Legislative Branches have acknowledged that the current system needs to be reviewed, and changes made where necessary. For example, President Bush outlined in the *National Strategy for Homeland Security* that "the threat of catastrophic terrorism requires a thorough review of the laws permitting the military to act within the United States in order to determine whether domestic preparedness and response efforts would benefit from greater involvement of military personnel and, if so, how." General Ralph Eberhart, former NORTHCOM Commander, said he "would favor changes in existing law [including the PCA] to give greater domestic powers to the military to protect the country against terrorist strikes." Senator John Warner, then-Chairman of the Senate Armed Services Committee, has also stated that "the reasons for the [PCA] have long given way to the changed lifestyle we face today here in America …" Clearly, there is considerable support to rescind or amend the PCA to allow DOD to take a more active role in the defense of the United States, including one of its most vulnerable domains: cyberspace.

There is a general consensus that the PCA is full of uncertainty and complexity. It is debatable when the PCA applies, what military activities are prohibited, and what boundaries for exceptions actually exist. All of this leaves policymakers, legal practitioners, lawmakers, and military personnel confused. This stems primarily from two reasons: (1) the difficulty in classifying situations as homeland defense or civil response and (2) misconceptions about the PCA due to the patchwork of legal

authorities in this area. The PCA is widely misunderstood and does not provide a basis for defining civil-military relations in the current War on Terror. It is time for the US to rescind the PCA and replace it with a new law. In critical situations like responding to nuclear terrorism or sophisticated cyber attacks, the current PCA interpretation can create a convoluted command and control structure, decrease response times, and increase continuity problems—leaving the federal response more vulnerable to exploitation. The PCA is irrelevant and even dangerous to the proper use of military forces for 21st century domestic duties such as cyber defense of national critical infrastructure. It is imperative that a new law provide clear guidelines for use of American military forces in homeland security duties, as well as enforcing US laws. One comprehensive statute could maintain the basic principles originally intended by the PCA, while setting clearer lines of demarcation between permissible and impermissible DOD activities.

Preparing to hit the 'send' button. (US Marine Corps)

DOD is Better Suited for Cyber Response

DOD can respond in the cyber arena in its area of expertise better than civilian authorities because cyber is at the core of the DOD mission. David McIntyre, the Director of the Integrative Center for Homeland Security at Texas A&M University, notes "the Pentagon's authority trumps that of DHS in the event of an attack …[and that] the Pentagon's role in a disaster leans heavily toward response and recovery, while DHS' is more focused on prevention and mitigation." Things should be no different in cyberspace. Cyber attacks need to be compared to vessels crossing into our territorial waters, or tanks rolling across the Mexican border. Arguably, any cyber attack that causes damage indistinguishable from a kinetic attack should be legally indistinguishable from more traditional military attacks.

The DOD should serve as the lead when necessary, as they are trained, equipped, and prepared to respond. In DOD's homeland defense role, the mission of "responding" is defined as "the ability to rapidly deter, repel, or defeat an attack." If deterrence fails, the military must be prepared to rapidly respond and defend against threats, including the use of preemptive or offensive actions such as computer network attack. Of course, it is still vital to work with and coordinate response capabilities with civilian counterparts as necessary. Furthermore, concerns that US service members will serve as a substitute for civilian law enforcement can be overcome through proper guidelines, and training to use the military in limited emergency circumstances.

Foreign vs Domestic Attacks

It is often too difficult to make distinctions between foreign and domestic attacks in cyberspace, so the military should be able to respond against both targets when necessary. The distinction between enemies at home and abroad has grown blurry in the information warfare age. Specifically, this new type of homeland defense must ignore the distinction between foreign and domestic threats to be successful, a fundamental difference found within the PCA. The 2003 *National Strategy to Secure Cyberspace* provides that "the speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which occurs only after the fact, if at all."

In most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of the attack, often making it impossible to determine at the outset if an intrusion is an act of vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage—or a strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from victim sites and intermediate sites, such as Internet Service Providers and telecommunications carriers.

Given the difficulty in determining the specific source of cyber attacks, it is arguable that unlike responding to traditional criminal acts, the focus should be on the act itself, rather than the perpetrator. Thus, the threshold for launching defensive and offensive actions should be lowered. Many cyber security experts agree it is hard to determine the origin of most cyber attacks due to the deliberately diffuse setup of the Internet. An attack that seems to emanate from one country can actually be controlled by another state, such as hijacking the victim's systems through a "botnet army" or other mechanisms.

Consequently, the PCA may need an additional exception carved out of the law, particularly for terrorist threats that law enforcement is not designed to handle, and when probable cause exists that those involved are foreign nationals or American citizens working on their behalf. Until we have the capabilities to determine cyber attack sources with the utmost confidence, such a solution is probably impractical. There are significant international law ramifications as well, such as what constitutes self-defense in cyberspace, and such issues still need work. Nonetheless, the PCA forces DOD to try to delineate between foreign and domestic sources, which is simply not possible—with reasonable certainty— before it is already too late.

Homeland Defense vs Homeland Security

Another distinction raising significant issues is trying to draw the line between permissible homeland defense and impermissible DOD homeland security operations in cyberspace. Joint Doctrine provides military support for homeland security in two ways: homeland defense and support to civil authorities with some of the relevant mission areas including: "sovereignty protection" (includes defense against CNA); protection of critical defense infrastructure; military assistance to civil authorities (includes CBRNE incidents); and military support to civilian law enforcement (includes combating terrorism and protecting critical national infrastructure). Under the current system, the military may not be able to adequately address a terrorist attack on American soil due to the lack of clear, explicit guidelines as to when the military should act, compounded by a cumbersome bureaucratic approval process. In addition to the President's ability to respond with military force to sudden attacks, without Congressional approval, it is arguable that lower level commanders could do likewise when faced with defending the homeland against a terrorist attack. However, terrorism is defined more as a law enforcement problem than a national security concern, and this limits DOD's ability to counter such actions in the United States.

If military activity falls under the realm of homeland defense or as part of a civil response not involving law enforcement activity, then it should be defendable under the PCA. Yet, the PCA tries to make distinctions between "military attacks" and "terrorist aggression" which are more theoretical than reality-based. DOD is supposed to be the lead agency for homeland defense missions. Consistent with law and policy, the Services support combatant command requirements against all incursions that threaten our national security, including computer network attack. Trying to draw lines between homeland defense and homeland security missions, in an effort to satisfy the PCA's requirements, does more harm than good in the event of a cyber attack.

Conclusions/Recommendations

Before a cyber attack does serious damage to US national security, whether against DOD or other national critical infrastructure, the United States needs to re-evaluate its policy and legal framework. We must enable this nation's response to the likely cyber challenges of the 21st century and beyond. After what may have been the first true "cyber war" in history—perhaps supported by Russia—Estonian Defense Minister Jack Aaviksoo warned:

...we haven't yet defined what can be considered to be a cyber attack, or what are the rights of member states and the obligations of EU and NATO in the event such attacks are launched. The EU and NATO need to work out a common legal basis to deal with cyberattacks. ... how to tackle different levels of criminal cyber-activities, depending on whether what we are dealing with is vandalism, cyber terror or cyber war. A "Pearl Harbor" in cyberspace could be devastating to US national security, and it should not be allowed to happen especially when it could have been prevented.

Accordingly, DOD should not only serve as the lead for cyber defense of defense critical infrastructure, it should also be in the lead for the response. This determination can be based on standards derived from the existing HSPD-7 or the *DOD Strategy for Homeland Defense and Civil Support*.

In addition, the PCA needs to be amended or rescinded. The PCA has "… succeeded in putting forth an ideal, but has fallen woefully short in creating a practical, legal impediment to the use of the military for civil law enforcement." The legal and policy arguments discussed in this article conclusively show this is the route we must take. Since it might be too sensitive a political issue to do away with the PCA completely, it could be more prudent to develop a new *DOD exception for cyberspace activities*. Again, such an exception could be based on the existing US government guidance and standards discussed earlier. Nonetheless, it would be very beneficial if all of the exceptions were combined with the PCA language into one comprehensive statute. Perhaps this can serve as another step toward dismantling the existing cumbersome structure—but only if the political will exists in the future. Too bad it's not as easy as a potential enemy's cyber attack, with one finger on a keyboard—just hit the "send" button.